Bounds for Robust Metering Schemes and Their Relationship with A^2-code

Wakaha Ogata[1] and Kaoru Kurosawa[2]

[1] Tokyo Institute of Technology, 2-12-1 O-okayama, Meguro-ku, Tokyo 152-8552, Japan
[2] Ibaraki University, 4-12-1 Nakanarusawa, Hitachi, Ibaraki, 316-8511, Japan

Abstract. A metering scheme allows a correct counting on the number of hits that a Web site received during a certain period. In this paper, we first derive tight lower bounds on the communication complexity $|V_i|$ $(i = 1, \ldots, n)$ and the size of server's secrets $|E_s|$ for robust and perfect (k, n)-metering schemes. We next show an almost equivalence between (k, n)-metering schemes and k-multiple-use A^2-codes. Finally, by using this equivalence, we derive lower bounds on $|V_i|$ and $|E_s|$ for robust (but not necessarily perfect) (k, n)-metering schemes.

1 Introduction

A (k, n)-metering scheme allows a correct counting on the number of hits that a Web site received during a certain period. That is, a Web server $\mathcal{S}$ can compute a *proof* if and only if k or more clients visited $\mathcal{S}$ during a certain period. Naor and Pinkas proposed the first cryptographically secure (k, n)-metering scheme [1]. Ogata and Kurosawa showed that their scheme is not as secure as they claimed and presented a more secure scheme [2].

More specifically, there exist four kinds of participants, a Web server $\mathcal{S}$, n clients $\mathcal{C}_1, \ldots, \mathcal{C}_n$, an audit agency $\mathcal{A}$ and an outside enemy $\mathcal{E}$ in this model. (We consider that n clients are monitors and the outside enemy is not.) We then require the following three kinds of security.

Security against servers A malicious Web server $\mathcal{S}$ tries to forge a *proof* from only $k-1$ or less shares (authenticators) of clients and to cheat $\mathcal{A}$. Hence $\mathcal{S}$ should not be able to inflate her hit counts. (There appears to be no way to detect whether $\mathcal{S}$ is deflating her hit counts.)

Security against clients Malicious clients try to forge an illegal share which would be accepted by $\mathcal{S}$, but would not allow $\mathcal{S}$ to compute the correct *proof*. Hence $\mathcal{S}$ must be able to detect illegal shares forged by clients.

Security against outside enemy An outside enemy $\mathcal{E}$ tries to forge a (legal or illegal) share which would be accepted by $\mathcal{S}$. If it is legal, it causes a counting error because he is not a monitor. If it is illegal, it does not allow $\mathcal{S}$ to compute the correct *proof*. Hence $\mathcal{S}$ must be able to detect a share forged by $\mathcal{E}$.

We say that a (k, n)-metering scheme is

- *robust* if it satisfies all the three security requirements.
- *non-robust* if it satisfies only the security against servers.

We further say that a (k, n)-metering scheme is perfect if $\mathcal{S}$ gains no information on *proof* from any $k-1$ or less shares. (It is interesting that the metering schemes proposed so far are all perfect.)

For *non*-robust and perfect metering schemes, a lower bound on the communication complexity $|V_i|$ $(i = 1, \ldots, n)$ was shown by De Bonis, B. Masucci [4] and by Masucci and Stinson [3], where V_i is a set of possible values v_i which is sent by client $\mathcal{C}_i$ to $\mathcal{S}$ when $\mathcal{C}_i$ has access to $\mathcal{S}$. (They considered a more general model than ours such that there are multiple Web servers and there exists a ramp structure among clients.)

However, *non*-robust metering schemes are not practical. We cannot assume that clients are all honest. We cannot assume that there is no outside enemy, either.

In this paper, we derive lower bounds on the communication complexity $|V_i|$ $(i = 1, \ldots, n)$ and the size of server's secrets $|E_s|$ for *robust* (k, n)-metering schemes.

We first derive lower bounds on $|V_i|$ and $|E_s|$ for "perfect and robust" (k, n)-metering schemes by using counting arguments. We also present a slightly modified version of the Ogata-Kurosawa scheme [2] and prove that it satisfies all the equalities of our bounds. This means that our bounds are all tight.

We next show an almost equivalence between robust (k, n)-metering schemes and k-multiple-use A^2-codes such that we can always construct a k-multiple-use A^2-code from a (k, n)-metering scheme, and in some cases, we can do the reverse. By using this equivalence, we derive lower bounds on $|V_i|$ and $|E_s|$ for robust (but not necessarily perfect) (k, n)-metering schemes. This equivalence is of independent interest because no relationship has been known between them so far.

	Lower bound on $\lvert V_i\rvert$	Lower bound on $\lvert E_s\rvert$
Non-robust and perfect	$[4, 3]$	Meaningless*
Robust and perfect	This paper	This paper
Robust	This paper	This paper

(For $*$, see the last paragraph of Sec.2.5.)

2 Preliminaries

2.1 Model of Metering Schemes

A (k, n)-metering scheme consists of three phases.

Initialization Phase: An audit agency $\mathcal{A}$ first generates a *proof*, a secret key e_s of the Web server $\mathcal{S}$ and a share v_i of client $\mathcal{C}_i$ for $i = 1, \ldots, n$. $\mathcal{A}$ then gives e_s to $\mathcal{S}$ and v_i to $\mathcal{C}_i$ for $i = 1, \ldots, n$ secretly.

Communication Phase: If $\mathcal{C}_i$ wants to see the Web page of $\mathcal{S}$, he sends v_i to $\mathcal{S}$. $\mathcal{S}$ accepts (i, v_i) iff $e_s(i, v_i) = 1$.

Proof Computing Phase: If k or more clients visited $\mathcal{S}$ during a certain period, then $\mathcal{S}$ can compute the *proof* from the k shares she received.

Let Proof, E_s and V_i be sets of possible values of the proof, server's key and $\mathcal{C}_i$'s share. It is desirable that $|E_s|$ and $|V_i|$ are small. Let $\widehat{\mathit{Proof}}, \hat{E}_s$ and $\hat{V}_i$ be the random variables distributed on Proof, E_s and V_i.

(k, n)-metering schemes must satisfy the security against malicious servers, the security against malicious clients and the security against outside enemies. These security are defined in the following subsections.

2.2 Security against Malicious Servers

A (k, n)-metering scheme must be secure at least against malicious servers. A malicious server tries to forge a *proof* from only $k-1$ shares of clients. Hence $\mathcal{S}$ should not be able to inflate her hit counts. (There appears to be no way to detect whether $\mathcal{S}$ is deflating her hit counts.)

Formally, a malicious $\mathcal{S}$ corrupts some $k-1$ clients $\mathcal{C}_{i_1}, \ldots, \mathcal{C}_{i_{k-1}}$ adaptively and then obtains their $k-1$ shares. $\mathcal{S}$ next forges a proof', hoping that $\mathit{proof}' = \mathit{proof}$. The cheating probability of this attack is defined by

$$P_S \stackrel{\triangle}{=} \max_{i_1,\ldots,i_{k-1}} \max_{\mathit{proof}'} \Pr(\widehat{\mathit{Proof}} = \mathit{proof}').$$

It is required that P_S is negligible in any metering scheme.

2.3 Perfect Metering Scheme

We say that a metering scheme is perfect if $\mathcal{S}$ gains no information on *proof* from any $k-1$ shares. Note that this is a stronger notion of security against server's attack than saying only that P_S is negligible.

Definition 1. *We say that a (k, n)-metering scheme is perfect if*

$$\Pr(\widehat{\mathit{Proof}} = \mathit{proof} \mid \hat{E}_s = e_s, \hat{V}_{i_1} = v_{i_1}, \ldots, \hat{V}_{i_{k-1}} = v_{i_{k-1}}) = \Pr(\widehat{\mathit{Proof}} = \mathit{proof}) \tag{1}$$

for any $e_s, v_{i_1}, \ldots, v_{i_{k-1}}$ and proof.

It is interesting that the metering schemes proposed so far are all perfect.

2.4 Robust Metering Scheme

We say that a metering scheme is robust if it is secure against malicious clients and outside enemies as well as malicious servers.

Malicious clients try to forge an illegal share which would be accepted by $\mathcal{S}$, but would not allow $\mathcal{S}$ to compute the correct *proof*. An outside enemy tries to forge a (legal or illegal) share which would be accepted by $\mathcal{S}$. If it is legal, it causes a counting error because he is not a monitor. If it is illegal, it does not allow $\mathcal{S}$ to compute the correct *proof*.

Clients' attack: Some (even all) clients collude and make a forged share $v_i' \neq v_i$ for some client $\mathcal{C}_i$. This attack will prevent $\mathcal{S}$ from computing the *proof* even if k or more clients visited $\mathcal{S}$. (For example, one illegal share and $k-1$ honest shares yield an illegal *proof* that is rejected by $\mathcal{A}$.) The cheating probability is defined by

$$P_C \stackrel{\triangle}{=} \max_{v_1,\ldots,v_n} \max_i \max_{v' \neq v_i} \Pr(\mathcal{S} \text{ accepts } (i, v') \mid v_1, \ldots, v_n \text{ are given}).$$

Outside enemy's attack: An outside enemy is interested in his attack before $\mathcal{S}$ computes a proof. Therefore, it must send the forged share to $\mathcal{S}$ before $\mathcal{S}$ receives k shares. In other words, the outside enemy can observe at most $k-1$ shares sent by clients before computing a forged share. To summarize, the outside enemy makes a forged share v_i' for some client $\mathcal{C}_i$ by observing $l < k$ shares of the other clients. The cheating probability of this attack is defined by

$$P_E \stackrel{\triangle}{=} \max_{0 \leq l < k} \max_{i_1,\ldots,i_l} \max_{v_{i_1},\ldots,v_{i_l}} \max_{i \notin \{i_1,\ldots,i_l\}, v'} \Pr(\mathcal{S} \text{ accepts } (i, v') \mid \mathcal{E} \text{ observes } v_{i_1}, \ldots, v_{i_l}).$$

A metering scheme is called robust if P_C and P_E are negligible.

2.5 Bounds for Non-robust Metering Scheme

A lower bound on the size of $|V_i|$ for non-robust and perfect metering schemes was shown by De Bonis, B. Masucci [4] and by Masucci and Stinson [3]. They considered a more general model than ours such that there are multiple servers.

Proposition 1. *[3, Corollary 3.9] In a non-robust and perfect (k, n)-metering scheme for multi servers,*

$$\log_2 |V_i| \geq H(\hat{V}_i) \geq sH(\widehat{Proof})$$

where s is the number of corrupted servers.

They also generalized their bound to ramp structures among clients.

In non-robust metering schemes, $\mathcal{S}$ does not need to have any $e_s \in E_s$ to check the shares of clients because there exist no malicious clients and outside enemies. Therefore, a lower bound on $|E_s|$ is meaningless in this case.

3 Bounds for "Perfect and Robust" Metering Scheme

Non-robust metering schemes are not practical. We cannot assume that clients are all honest. We cannot assume that there is no outside enemy, either.

In this section, we derive a lower bound on $|V_i|$ and a lower bound on $|E_s|$ for *perfect and robust* (k, n)-metering schemes. We also present a slightly modified version of the Ogata-Kurosawa scheme [2] and prove that it satisfies all the equalities of our bounds. This means that our bounds are all tight.

3.1 Lower bound on $|V_i|$

Fix $i_1, \ldots, i_k$ arbitrarily. For each $1 \le l \le k$, define

$$V_{i_l}(e_s, v_{i_1}, \ldots, v_{i_{l-1}}) \stackrel{\triangle}{=} \{v_{i_l} \mid \Pr(\hat{E}_s = e_s, \hat{V}_{i_1} = v_{i_1}, \ldots, \hat{V}_{i_{l-1}} = v_{i_{l-1}}, \hat{V}_{i_l} = v_{i_l}) > 0\},$$
$$V_{i_l}(v_{i_1}, \ldots, v_{i_{l-1}}) \stackrel{\triangle}{=} \{v_{i_l} \mid \Pr(\hat{V}_{i_1} = v_{i_1}, \ldots, \hat{V}_{i_{l-1}} = v_{i_{l-1}}, \hat{V}_{i_l} = v_{i_l}) > 0\},$$
$$E_s(v_{i_1}, \ldots, v_{i_l}) \stackrel{\triangle}{=} \{e_s \mid \Pr(\hat{E}_s = e_s, \hat{V}_{i_1} = v_{i_1}, \ldots, \hat{V}_{i_l} = v_{i_l}) > 0\}.$$

Note that $V_{i_k} \supseteq V_{i_k}(e_s) \supseteq \cdots \supseteq V_{i_k}(e_s, v_{i_1}, \ldots, v_{i_{k-1}})$.

Lemma 1. *For any possible $e_s, v_{i_1}, \ldots, v_{i_{k-1}}$,*

$$|V_{i_k}(e_s, v_{i_1}, \ldots, v_{i_{k-1}})| \ge |Proof|.$$

Proof. Fix any possible $e_s, v_{i_1}, \ldots, v_{i_{k-1}}$ arbitrarily. Then any $proof \in Proof$ can happen with positive probability in a perfect (k, n)-metering scheme. On the other hand, each $v_{i_k} \in V_{i_k}(e_s, v_{i_1}, \ldots, v_{i_{k-1}})$ must determine $proof \in Proof$ uniquely. This means that there exists an onto mapping from $V_{i_k}(e_s, v_{i_1}, \ldots, v_{i_{k-1}})$ to $Proof$. Therefore,

$$|V_{i_k}(e_s, v_{i_1}, \ldots, v_{i_{k-1}})| \ge |Proof|.$$

□

Corollary 1. *$|V_i(e_s)| \ge |Proof|$ for any i.*

Theorem 1. *In a perfect and robust (k, n)-metering scheme,*

$$|V_i| \ge |Proof|(P_E)^{-1}$$

for any i.

Proof. We will derive a lower bound on P_E. Define

$$\phi(e_s, v_i) \stackrel{\triangle}{=} \begin{cases} 1 \text{ if } v_i \in V_i(e_s) \\ 0 \text{ otherwise.} \end{cases}$$

Note that $\mathcal{S}$ accepts (i, v_i) iff $v_i \in V_i(e_s)$. Therefore,

$$\begin{aligned} \sum_{v_i \in V_i} \Pr(\mathcal{S} \text{ accepts } (i, v_i)) &= \sum_{v_i \in V_i} \sum_{e_s \in E_s} \Pr(e_s)\phi(e_s, v_i) \\ &= \sum_{e_s \in E_s} \Pr(e_s) \sum_{v_i \in V_i} \phi(e_s, v_i) \\ &= \sum_{e_s \in E_s} \Pr(e_s)|V_i(e_s)| \\ &\ge |Proof| \sum_{e_s \in E_s} \Pr(e_s) \qquad \text{(from Corollary 1)} \\ &= |Proof|. \end{aligned}$$

Therefore,

$$P_E \ge \max_{v_i \in V_i} \Pr(\mathcal{S} \text{ accepts } (i, v_i)) \ge |Proof|/|V_i|.$$

□

3.2 Lower bound on $|E_s|$

Define

$$ALL \stackrel{\triangle}{=} \{(v_1,\ldots,v_k) \mid \Pr(\hat{V}_1 = v_1,\ldots,\hat{V}_k = v_k) > 0\},$$
$$ALL(e_s) \stackrel{\triangle}{=} \{(v_1,\ldots,v_k) \mid \Pr(\hat{E}_s = e_s, \hat{V}_1 = v_1,\ldots,\hat{V}_k = v_k) > 0\}.$$

Lemma 2. *If the equality of corollary 1 holds for all i, then*

$$|ALL(e_s)| = |Proof|^k.$$

Proof. From the equality of Corollary 1 and Lemma 1,

$$|Proof| = |V_2(e_s)| \geq |V_2(e_s, v_1)| \geq |Proof|.$$

Therefore, $|V_2(e_s, v_1)| = |Proof|$ for any $v_1 \in V_1(e_s)$. Hence,

$$|\{(v_1, v_2) \mid \Pr(\hat{E}_s = e_s, \hat{V}_1 = v_1, \hat{V}_2 = v_2) > 0\}| = |V_1(e_s)| \times |V_2(e_s, v_1)| = |Proof|^2.$$

By repeating this process, we have $|ALL(e_s)| = |Proof|^k$. □

Lemma 3. $|V_{i_{l+1}}(v_{i_1},\ldots,v_{i_l})| \geq |Proof|(P_E)^{-1}$ *for* $1 \leq l \leq k-1$.

Proof. Similar to the proof of Theorem 1. Suppose that an outside enemy $\mathcal{E}$ observes l shares sent by clients, say $\mathcal{C}_{i_1},\ldots,\mathcal{C}_{i_l}$. Let their shares be $\vec{v} = (v_{i_1},\ldots,v_{i_l})$. Define

$$\phi(e_s, v_{i_{l+1}}) \stackrel{\triangle}{=} \begin{cases} 1 \text{ if } v_{i_{l+1}} \in V_{i_{l+1}}(e_s) \\ 0 \text{ otherwise.} \end{cases}$$

Note that $\mathcal{S}$ accepts $(i_{l+1}, v_{i_{l+1}})$ iff $v_{i_{l+1}} \in V_{i_{l+1}}(e_s)$. Therefore,

$$\begin{aligned}
&\sum_{v_{i_{l+1}} \in V_{i_{l+1}}(\vec{v})} \Pr(\mathcal{S} \text{ accepts } (i_{l+1}, v_{i_{l+1}}) \mid \mathcal{E} \text{ observes } \vec{v}) \\
&= \sum_{v_{i_{l+1}} \in V_{i_{l+1}}(\vec{v})} \sum_{e_s \in E_s(\vec{v})} \Pr(e_s \mid \vec{v}) \phi(e_s, v_{i_{l+1}}) \\
&= \sum_{e_s \in E_s(\vec{v})} \Pr(e_s \mid \vec{v}) \sum_{v_{i_{l+1}} \in V_{i_{l+1}}(\vec{v})} \phi(e_s, v_{i_{l+1}}) \\
&= \sum_{e_s \in E_s(\vec{v})} \Pr(e_s \mid \vec{v}) |V_{i_{l+1}}(\vec{v}) \cap V_{i_{l+1}}(e_s)| \\
&= \sum_{e_s \in E_s(\vec{v})} \Pr(e_s \mid \vec{v}) |V_{i_{l+1}}(e_s, \vec{v})| \\
&\geq |Proof| \sum_{e_s \in E_s(\vec{v})} \Pr(e_s \mid \vec{v}) \qquad \text{(from Lemma 1)} \\
&= |Proof|.
\end{aligned}$$

Therefore,

$$P_E \geq |Proof| / |V_{i_{l+1}}(\vec{v})|.$$

□

Lemma 4. $|E_s(v_1, \ldots, v_k)| \geq P_C^{-1}$.

Proof. Consider the following attack of k clients $\mathcal{C}_1, \ldots, \mathcal{C}_k$. Let their shares be $\vec{v} = (v_1, \ldots, v_k)$. First, they choose $e'_s \in E_s(\vec{v})$ such that

$$\Pr(e'_s \mid \vec{v}) = \max_{e_s \in E_s(\vec{v})} \Pr(e_s \mid \vec{v}).$$

Next they choose v'_1 randomly from $V_1(e'_s, v_2, \ldots, v_k) \setminus \{v_1\}$. Finally $\mathcal{C}_1$ sends v'_1 to $\mathcal{S}$. Clearly, this attack succeeds if $\mathcal{S}$ has e'_s. Therefore,

$$P_C \geq \Pr(\mathcal{S} \text{ has } e'_s \mid \vec{v}) = \max_{e_s \in E_s(\vec{v})} \Pr(e_s \mid \vec{v}) \geq 1/|E_s(\vec{v})|.$$

□

Lemma 5. $|ALL| \geq |Proof|^k (P_E^k)^{-1}$.

Proof. First from Theorem 1,

$$|V_1| \geq |Proof|(P_E)^{-1}.$$

Next from Lemma 3,

$$|V_2(v_1)| \geq |Proof|(P_E)^{-1}$$

for each $v_1 \in V_1$. Therefore,

$$|\{(v_1, v_2) \mid \Pr(\hat{V}_1 = v_1, \hat{V}_2 = v_2) > 0\}| \geq |Proof|^2 (P_E^2)^{-1}.$$

By repeating this process, we obtain that $|ALL| \geq |Proof|^k (P_E^k)^{-1}$. □

Theorem 2. *Suppose that the equality of Corollary 1 holds for all i and e_s. Then in a perfect and robust (k, n)-metering scheme,*

$$|E_s| \geq (P_C P_E^k)^{-1}.$$

Proof. First from Lemma 2,

$$\sum_{e_s \in E_s} |ALL(e_s)| = |E_s||Proof|^k.$$

Next

$$\begin{aligned} \sum_{(v_1,\ldots,v_k)} |E_s(v_1, \ldots, v_k)| &\geq |ALL| P_C^{-1} && \text{(Lemma 4)} \\ &\geq |Proof|^k (P_E^k)^{-1} (P_C)^{-1} && \text{(Lemma 5)}. \end{aligned}$$

On the other hand, it is easy to see that

$$\sum_{e_s \in E_s} |ALL(e_s)| = \sum_{(v_1,\ldots,v_k)} |E_s(v_1, \ldots, v_k)|.$$

Therefore,

$$|E_s| \geq \frac{|Proof|^k (P_E^k)^{-1} (P_C)^{-1}}{|Proof|^k} = (P_E^k P_C)^{-1}.$$

□

3.3 Modified Ogata-Kurosawa scheme

We next present a slightly modified version of the Ogata-Kurosawa scheme [2] and prove that it satisfies all the equalities of our bounds. This means that our bounds are all tight.

The modified Ogata-Kurosawa scheme is described as follows. Let $p > n$ be a large prime number.

Initialization Phase: 1. An audit agency $\mathcal{A}$ chooses a random number $r \in Z_p$ and two random polynomials $f_0(y)$ and $f_1(y)$ with degree at most $k-1$ over $GF(p)$.
2. Let $proof = f_1(0)$.
3. $\mathcal{A}$ gives $e_s = (r, g(y))$ to the Web server $\mathcal{S}$, where

$$g(y) = f_0(y) + r f_1(y).$$

4. $\mathcal{A}$ gives $v_i = (f_0(i), f_1(i))$ to client $\mathcal{C}_i$ for $1 \le i \le n$.

Communication Phase: If $\mathcal{C}_i$ wants to see the Web page of $\mathcal{S}$, he sends $v_i = (a, b)$ to $\mathcal{S}$. $\mathcal{S}$ accepts $(i, (a, b))$ iff

$$g(i) = a + rb. \tag{2}$$

Proof Computing Phase: If k or more clients visited $\mathcal{S}$, then $\mathcal{S}$ can compute $proof = f_1(0)$ by using Lagrange formula.

In the above scheme, it is clear that

$$|Proof| = p, \quad |E_s| = p^{k+1}, \quad |V_i| = p^2$$

for each i. We then prove the following theorem.

Theorem 3. *The modified Ogata-Kurosawa scheme is perfect and*

$$P_C = P_E = 1/p. \tag{3}$$

Proof. Note that the secret key of $\mathcal{A}$ is $K = (r, f_0(y), f_1(y))$.

1. For simplicity, let $i_1 = 1, \ldots, i_{k-1} = k-1$. Fix

$$e_s = (r, g(y)), v_1 = (a_1, b_1), \ldots, v_{k-1} = (a_{k-1}, b_{k-1})$$

arbitrarily. We will show that there exists a unique $(f_0(y), f_1(y))$ for each value of $proof$. Fix $proof$ arbitrarily. First there exists a unique $f_1(y)$ such that

$$f_1(0) = proof, f_1(1) = b_1, \ldots, f_1(k-1) = b_{k-1}$$

because $\deg(f_1)$ is at most $k-1$. Next $f_0(y)$ is uniquely determined as

$$f_0(y) = g(y) - r f_1(y)$$

because $e_s = (r, g(y))$ is fixed. Therefore, each value of $proof$ is equally likely to happen for any fixed $e_s, v_1, \ldots, v_{k-1}$. This means that

$$\Pr(\widehat{Proof} = proof \mid e_s, v_1, \ldots, v_{k-1}) = 1/p = \Pr(\widehat{Proof} = proof).$$

Hence the scheme is perfect.

2. Fix
$$v_1 = (a_1, b_1), \ldots, v_n = (a_n, b_n) \tag{4}$$
and $i \in \{1, \ldots, n\}$ arbitrarily. Let B_0 be the set of $K = (r, f_0(y), f_1(y))$ such that eq.(4) holds. For $v' = (a', b')$ such that $(a', b') \neq (a_i, b_i)$, let B_1 be a subset of B_0 such that $\mathcal{S}$ accepts (i, v'). Then
$$P_C = \max \Pr(\mathcal{S} \text{ accepts } (i, v') \mid v_1, \ldots, v_n) = \max |B_1|/|B_0|.$$
We will compute $|B_0|$ and $|B_1|$. First since $f_0(y)$ and $f_1(y)$ are uniquely determined from eq.(4), we have
$$|B_0| = |\{r\}| = p.$$
Next since $\mathcal{S}$ accepts (i, v'), $g(i) = a' + rb'$. On the other hand, from eq.(2), $g(i) = a_i + rb_i$. Therefore,
$$a_i + rb_i = a' + rb',$$
$$r(b_i - b') = a' - a_i.$$
The above equation has at most one solution on r because $(a', b') \neq (a_i, b_i)$. Therefore, $\max |B_1| = 1$. Hence
$$P_C = \max |B_1|/|B_0| = 1/p.$$
3. For simplicity, let $l = k - 1$ and $i_1 = 1, \ldots, i_{k-1} = k - 1$. Fix
$$v_1 = (a_1, b_1), \ldots, v_{k-1} = (a_{k-1}, b_{k-1}) \tag{5}$$
and $i (\geq k)$ arbitrarily. Let B_0 be the set of $K = (r, f_0(y), f_1(y))$ such that eq.(5) holds. For $v' = (a', b')$ let B_1 be a subset of B_0 such that $\mathcal{S}$ accepts (i, v'). Then
$$P_E = \max \Pr(\mathcal{S} \text{ accepts } (i, v') \mid v_1, \ldots, v_{k-1}) = \max |B_1|/|B_0|.$$
We will compute $|B_0|$ and $|B_1|$. First since $f_0(y)$ and $f_1(y)$ are uniquely determined from the values of $f_0(0)$ and $f_1(0)$, we have
$$|B_0| = |\{r, f_0(0), f_1(0)\}| = p^3.$$
Next $g(i) = a' + rb'$ if $\mathcal{S}$ accepts (i, v'). On the other hand, $g(i) = f_0(i) + rf_1(i)$. Therefore,
$$f_0(i) + rf_1(i) = a' + rb'.$$
In the above equation, $f_0(i)$ is uniquely determined from each values of $(r, f_1(i))$. (Note that $f_0(y)$ and $f_1(y)$ are uniquely determined from each values of $f_0(i)$ and $f_1(i)$.) Therefore,
$$|B_1| = |\{r, f_1(i)\}| = p^2.$$
Hence
$$P_E = \max |B_1|/|B_0| = 1/p.$$

□

It is now easy to see that all the equalities of our bounds are satisfied by the above scheme.

(Remark) In the original Ogata-Kurosawa scheme, $proof = f_0(0)$ and r is randomly chosen from $Z_p \setminus \{0\}$. Therefore, $P_C = 1/(p-1)$ and $|E_s| = (p-1)p^k$.

4 Lower Bounds for Multiple-use A^2-code

For multiple-use A^2-codes, Wang. et.al. derived a lower bound on the cheating probabilities and a lower bound on the size of keys [8]. (See Appendix A.) However, their bound on the size of keys holds under the condition that the cheating probabilities satisfy their lower bound (see Proposition 3). We can not derive a lower bound on the size of authenticators from their result, either.

In this section, we first define the cheating probabilities in a different way from [8]. We then derive a lower bound on the size of keys which holds for any values of the cheating probabilities. We derive a lower bound on the size of authenticators, also.

The result of this section will be used in the following sections.

4.1 Multiple-use A^2-code

In the model for unconditionally secure authentication codes (A-codes), the transmitter $\mathcal{T}$ and the receiver $\mathcal{R}$ use the same encoding rule to protect their communication from deception of an outside enemy $\mathcal{O}$.

An authentication code with arbitration (A^2-code) enables to authenticate a message sent by $\mathcal{T}$ to $\mathcal{R}$ even if $\mathcal{T}$ and $\mathcal{R}$ do not trust each other [6, 7]. A^2-code includes the fourth person called an *arbiter* $\mathcal{A}'$, who solves disputes between $\mathcal{T}$ and $\mathcal{R}$.

In this paper, we consider A^2-codes which are used to send multiple messages. If $\mathcal{T}$ can use an A^2-code to send $k-1$ messages to $\mathcal{R}$ which are authenticated, then we call the code *a k-multiple-use A^2-code.*

A k-multiple-use A^2-code consists of three phases.

Initialization Phase: An arbiter $\mathcal{A}'$ first generates a secret key e_t of $\mathcal{T}$ and a secret key e_r of $\mathcal{R}$. $\mathcal{A}'$ then gives e_t to $\mathcal{T}$ and e_r to $\mathcal{R}$ secretly.

Communication Phase: For a source state s, $\mathcal{T}$ computes an authenticator $a = e_t(s)$. $\mathcal{T}$ then sends $m = (s, a)$ to $\mathcal{R}$, where m is called a message. $\mathcal{R}$ accepts $m = (s, a)$ as authentic iff $e_r(s, a) = 1$.

Dispute Phase: On dispute between $\mathcal{T}$ and $\mathcal{R}$, $\mathcal{A}'$ accepts $m = (s, a)$ as authentic iff $a = e_t(s)$.

Define $E_t \overset{\triangle}{=} \{e_t\}, E_r \overset{\triangle}{=} \{e_r\}, M \overset{\triangle}{=} \{m\}, S \overset{\triangle}{=} \{s\}$ and $A \overset{\triangle}{=} \{a\}$. Let $\hat{E}_t, \hat{E}_r, \hat{M}, \hat{S}, \hat{A}$ be the random variables distributed over E_t, E_r, M, S, A, respectively.

In the model of k-multiple-use A^2-codes, there are three kinds of attacks.

Transmitter's attack: $\mathcal{T}$ sends a message $m = (s, a)$ to the receiver $\mathcal{R}$ and denies having sent it. $\mathcal{T}$ successes if m is accepted by $\mathcal{R}$ as authentic and $a \neq e_t(s)$.

Receiver's attack: $\mathcal{R}$ receives less than k messages and claims to have received a new message $m' = (s', a')$. $\mathcal{R}$ successes if $a' = e_t(s')$.

Outside enemy's attack: An outside enemy $\mathcal{O}$ observes $i < k$ messages sent by $\mathcal{T}$, and then substitutes the last one with a forged one $m' = (s', a')$. $\mathcal{O}$ successes if $e_r(s', a') = 1$.

We define the cheating probabilities of k-multiple-use A^2-code as follows, where P_T, P_{R_i} and P_{O_i} denote the cheating probabilities by $\mathcal{T}$, $\mathcal{R}$ and $\mathcal{O}$, respectively.

$$P_T \triangleq E\left(\max_{m=(s,a), a\neq e_t(s)} \Pr(e_r(s,a)=1)\right)$$

$$P_{R_i} \triangleq E\left(\max_{(s',a')\notin\{m_1,\ldots,m_i\}} \Pr(a' = e_t(s') \mid \mathcal{T} \text{ sent } m_1, \ldots, m_i)\right)$$

$$P_{O_i} \triangleq E\left(\max_{m'\notin\{m_1,\ldots,m_i\}} \Pr(\mathcal{R} \text{ accepts } m' \mid \mathcal{T} \text{ sent } m_1, \ldots, m_i)\right),$$

where $0 \leq i \leq k-1$. Let

$$P_O \triangleq \max_{0\leq i<k} P_{O_i}, \quad P_R \triangleq \max_{0\leq i<k} P_{R_i}.$$

4.2 Lower Bounds

In this subsection, we present a lower bound on the cheating probabilities defined as above. It is a generalization of a lower bound for usual A^2-codes given by Johansson [10].

Theorem 4.

$$P_T \geq 2^{-H(\hat{E}_r|\hat{E}_t)}$$

$$P_{R_i} \geq 2^{-H(\hat{E}_t|\hat{M}_1\cdots\hat{M}_i,\hat{E}_r)+H(\hat{E}_t|\hat{M}_1\cdots\hat{M}_{i+1},\hat{E}_r)}$$

$$P_{O_i} \geq 2^{-I(\hat{E}_r;\hat{E}_t|\hat{M}_1\cdots\hat{M}_i)+I(\hat{E}_r;\hat{E}_t|\hat{M}_1\cdots\hat{M}_{i+1})}$$

The proof will be given in the final paper. We then obtain a lower bound on the size of keys as follows.

Theorem 5. *If $\hat{S}$ is uniformly distributed, then*

$$|E_t| \geq (P_R P_O)^{-k}, \quad |E_r| \geq (P_T P_O^k)^{-1}, \quad |A| \geq (P_R P_O)^{-1}.$$

Proof. From Theorem 4,

$$(P_R)^k \geq (P_{R_0} \cdots P_{R_{k-1}}) \geq 2^{-H(\hat{E}_t|\hat{E}_r)+H(\hat{E}_t|\hat{M}_1\cdots\hat{M}_k,\hat{E}_r)}$$
$$(P_O)^k \geq (P_{O_0} \cdots P_{O_{k-1}}) \geq 2^{-I(\hat{E}_t;\hat{E}_r)+I(\hat{E}_t;\hat{E}_r|\hat{M}_1\cdots\hat{M}_k)}$$
$$(P_O P_R)^k \geq 2^{-H(\hat{E}_t)+H(\hat{E}_t|\hat{M}_1\cdots\hat{M}_k)}$$
$$\geq 2^{-H(\hat{E}_t)},$$
$$|E_t| \geq 2^{H(\hat{E}_t)} \geq (P_O P_R)^{-k}.$$

The second bound can be derived similarly.

The bound on $|A|$ is derived as follows.

$$|M| \geq 2^{H(\hat{M}|\hat{E}_r)+I(\hat{M};\hat{E}_r)}$$
$$= 2^{H(\hat{M}|\hat{E}_r)} 2^{I(\hat{M};\hat{E}_r;\hat{E}_t)} 2^{I(\hat{M};\hat{E}_t|\hat{E}_r)}$$
$$\geq 2^{H(\hat{S})} 2^{I(\hat{E}_r;\hat{E}_t)-I(\hat{E}_r;\hat{E}_t|\hat{M})} 2^{H(\hat{E}_t|\hat{E}_r)-H(\hat{E}_t|\hat{M},\hat{E}_r)}$$

From Theorem 4, it holds that

$$2^{I(\hat{E}_r;\hat{E}_t)-I(\hat{E}_r;\hat{E}_t|\hat{M})} \geq 1/P_{O_0},$$
$$2^{H(\hat{E}_t|\hat{E}_r)-H(\hat{E}_t|\hat{M},\hat{E}_r)} \geq 1/P_{R_0}.$$

Therefore,

$$|M| \geq 2^{H(\hat{S})}/P_{O_0}P_{R_0} = |S|/P_{O_0}P_{R_0},$$
$$|A| = |M|/|S| \geq (P_O P_R)^{-1}.$$

□

We can see that the above bounds are tight because there exists an A^2-code which satisfies all the equalities of them (see appendix B).

5 Almost Equivalence

In this section, we show an almost equivalence between robust (k,n)-metering schemes and k-multiple-use A^2-codes such that we can always construct a k-multiple-use A^2-code from a (k,n)-metering scheme, and in some cases, we can do the reverse.

In what follows, we define the cheating probability of clients and the cheating probability of outside enemies as follows.

$$\tilde{P}_C \stackrel{\triangle}{=} E\left(\max_i \max_{v_i' \neq v_i} \Pr(\mathcal{S} \text{ accepts } (i, v_i') \mid v_1, \ldots, v_n \text{ are given})\right),$$

where E is taken over $v_1, \ldots, v_n$.

$$\tilde{P}_E \stackrel{\triangle}{=} \max_{0 \leq l < k} E\left(\max_{i \notin \{i_1,\ldots,i_l\}, v_i'} \Pr(\mathcal{S} \text{ accepts } (i, v_i') \mid \mathcal{E} \text{ observes } v_{i_1}, \ldots, v_{i_l})\right),$$

where E is taken over $i_1, \ldots, i_l$ and $v_{i_1}, \ldots, v_{i_l}$.

The cheating probabilities of k-multiple-use A^2-codes are defined in the previous section.

5.1 Metering Scheme Implies a Multiple-use A^2-code

First, we show that a (k,n)-metering scheme implies a k-multiple-use A^2-code. Wlog, suppose that $V_i \subseteq V$, where $|V| = \max_i |V_i|$.

Theorem 6. *If there exists a* (k,n)*-metering scheme with* $(\mathit{Proof}, E_s, \{V_i\})$ *and* $(\tilde{P}_C, P_S, \tilde{P}_E)$*, then there exists a* k*-multiple-use* A^2*-code with* (E_t, E_r, S, A) *and* (P_T, P_R, P_O) *such that*

$$P_T = \tilde{P}_C, \quad P_R \leq P_S, \quad P_O = \tilde{P}_E,$$
$$E_t = V_1 \times \cdots \times V_n, \quad E_r = E_s, \quad S = \{1, 2, \ldots, n\}, \quad A = V.$$

Proof. Suppose that there exists a (k,n)-metering scheme with $(\mathit{Proof}, E_s, \{V_i\})$ and $(\tilde{P}_C, P_S, \tilde{P}_E)$. We then construct a k-multiple-use A^2-code as follows.

Initialization Phase: The arbiter $\mathcal{A}'$ first runs the audit agency $\mathcal{A}$ of the (k,n)-metering scheme to generate *proof*, e_s and $(v_1, \ldots, v_n)$. $\mathcal{A}'$ then gives $e_t \stackrel{\triangle}{=} (v_1, \ldots, v_n)$ to $\mathcal{T}$ and $e_r \stackrel{\triangle}{=} e_s$ to $\mathcal{R}$ secretly as their secret keys.

Communication Phase: For a source state $i \in \{1, \ldots, n\}$, $\mathcal{T}$ sends a message $m = (i, v_i)$ to $\mathcal{R}$, where v_i is the authenticator for i.

Dispute Phase: On dispute between $\mathcal{T}$ and $\mathcal{R}$, $\mathcal{A}'$ accepts $m = (i, a)$ as authentic iff $a = v_i$.

It is clear that $E_t = V_1 \times \cdots \times V_n, E_r = E_s, S = \{1, 2, \ldots, n\}, A = V$.

Next it is easy to see that an outside enemy's attack on the (k,n)-metering scheme can be directly used as an outside enemy's attack on the k-multiple-use A^2-code and vice versa. Therefore, $P_O = \tilde{P}_E$.

A clients' attack on the (k,n)-metering scheme is that all clients collude and make a forged share $v_s' \neq v_s$. In other words, from given $(1, v_1), \ldots, (n, v_n)$, they make $v_s' \neq v_s$ for some s, hoping that it is accepted by $\mathcal{S}$ with her secret key e_s. Then it is easy to see that this attack can be directly used as a transmitter's attack on the k-multiple-use A^2-code. Therefore, $P_T \geq \tilde{P}_C$. It is easy to see that the converse part is also true. Hence $\tilde{P}_C \geq P_T$. Therefore, $P_T = \tilde{P}_C$.

Suppose that there exists a receiver's attack R_{attack} on the k-multiple-use A^2-code with success probability P_R. Then we consider a server's attack on the (k,n)-metering scheme as follows. Suppose that $l < k$ clients $\mathcal{C}_{i_1}, \ldots, \mathcal{C}_{i_l}$ visited $\mathcal{S}$. $\mathcal{S}$ runs R_{attack} on input e_r and l messages $(i_1, v_{i_1}), \ldots, (i_l, v_{i_l})$. R_{attack} outputs a new message $m = (s, v_s)$ for some $s \notin \{i_1, \ldots, i_l\}$. $\mathcal{S}$ next corrupts $k - l - 1$ clients $\mathcal{C}_{i_{l+1}}, \ldots, \mathcal{C}_{i_{k-1}}$ other than $\{i_1, \ldots, i_l, s\}$ and obtains their shares. Then $\mathcal{S}$ obtains k shares $v_{i_1}, \ldots, v_{i_{k-1}}$ and v_s in total. Therefore, $\mathcal{S}$ can compute the *proof* from the k shares. This attack succeeds with probability P_R. Hence, $P_S \geq P_R$. $\square$

5.2 Weak converse

Next, we show a weak converse of Theorem 6.

Lemma 6. *In a k-multiple-use A^2-code in which $|E_t|$ satisfies the equality of the bound in Theorem 5, the transmitter's key is determined uniquely from k or more valid messages.*

Proof. From the proof of Theorem 5, We obtain

$$(P_O P_R)^k \geq 2^{-H(\hat{E}_t)+H(\hat{E}_t|\hat{M}_1 \cdots \hat{M}_k)}.$$

The equality of the bound holds only if $H(\hat{E}_t \mid \hat{M}_1 \cdots \hat{M}_k) = 0$. This means that e_t is determined by k messages. □

Theorem 7. *If there exists a k-multiple-use A^2-code with (E_t, E_r, S, A) and (P_T, P_R, P_O) such that $|E_t|$ satisfies the equality of the bound in Theorem 5, then there exists a (k,n)-metering scheme with $(Proof, E_s, \{V_i\})$ and $(\tilde{P}_C, P_S, \tilde{P}_E)$, such that*

$$\begin{aligned} &\tilde{P}_C = P_T,\ \ P_S \leq P_R, \quad \tilde{P}_E = P_O \\ &E_s = E_r,\ \ n = |S| - 1, \quad Proof = V_1 = \cdots = V_n = A. \end{aligned}$$

Proof. (Sketch) Using a k-multiple-use A^2-code, construct a metering scheme described as follows. $\mathcal{A}$ chooses $s_0 \in S$ and sets $proof = e_t(s_0)$. Each client $\mathcal{C}_i$ receives $v_i = e_t(s_i)$ where $S = \{s_0, \ldots, s_n\}$.

If $|E_t|$ satisfies the equality of the bound, e_t is determined uniquely from k or more valid messages (from Lemma 6). Then the server can obtain $proof = e_t(s_0)$ if he has been visited by k or more clients. The rest of the proof is similar to Theorem 6. □

6 Lower Bounds for Robust Metering Scheme

In this section, we derive a lower bound on $|V_i|$ and a lower bound on $|E_s|$ for robust (but not necessarily perfect) (k,n)-metering schemes by using our relationship between metering schemes and multiple A^2-codes (and our lower bounds for k-multiple-use A^2-codes of Sec.4).

6.1 Bounds for Robust Metering Schemes

From Theorem 5 and Theorem 6, we immediately obtain a lower bound on the size of keys for (k,n)-metering schemes as follows.

Corollary 2. *In a (k,n)-metering scheme, if each client visits the Web sever $\mathcal{S}$ with equal probability, then*

$$\max_i |V_i| \geq (P_S \tilde{P}_E)^{-1}, \quad |E_s| \geq (\tilde{P}_C \tilde{P}_E^k)^{-1}.$$

Corollary 2 is tight because the Ogata-Kurosawa metering scheme satisfies all the equalities of the bound (see Sec.3.3).

6.2 Bound on $\tilde{P}_E$

We can remove $\tilde{P}_E$ from the above bound by using Theorem 8.

Theorem 8. *In a (k, n)-metering scheme,*

$$\tilde{P}_E \leq \tilde{P}_C + P_S.$$

Proof. (Sketch) From the definition of $\tilde{P}_E$,

$$\tilde{P}_E \leq \max_l E\left(\max_{i,v'_i} \Pr(\mathcal{S} \text{ accepts } (i, v'_i) \wedge \mathcal{C}_i \text{ has } v'_i \mid \mathcal{S} \text{ observes } v_{i_1}, \ldots, v_{i_l})\right)$$
$$+ \max_l E\left(\max_{i,v'_i} \Pr(\mathcal{S} \text{ accepts } (i, v'_i) \wedge \neg(\mathcal{C}_i \text{ has } v'_i) \mid \mathcal{S} \text{ observes } v_{i_1}, \ldots, v_{i_l})\right).$$

The first term of the right hand is equal or less than P_S, while the second term is equal or less than $\tilde{P}_C$. □

Corollary 3. *In a (k, n)-metering scheme, if each client visits the Web sever $\mathcal{S}$ with equal probability, then*

$$\max_i |V_i| \geq (P_S(P_S + \tilde{P}_C))^{-1}, \quad |E_s| \geq (\tilde{P}_C(P_S + \tilde{P}_C)^k)^{-1}.$$

7 Conclusion

In this paper, We first derived lower bounds on $|V_i|$ and $|E_s|$ for "perfect and robust" (k, n)-metering schemes by using counting arguments, where $|V_i|$ $(i = 1, \ldots, n)$ is the communication complexity and and $|E_s|$ is the size of server's secrets. We also presented a slightly modified version of the Ogata-Kurosawa scheme [2] and proved that it satisfies all the equalities of our bounds. This means that our bounds are all tight.

We next showed an almost equivalence between robust (k, n)-metering schemes and k-multiple-use A^2-codes such that we can always construct a k-multiple-use A^2-code from a (k, n)-metering scheme, and in some cases, we can do the reverse. By using this equivalence, we derived lower bounds on $|V_i|$ and $|E_s|$ for robust (but not necessarily perfect) (k, n)-metering schemes. This equivalence is of independent interest because no relationship has been known between them so far.

References

1. M. Naor and B. Pinkas, "Secure and Efficient Metering," Proc. of Eurocrypt '98, Lecture Notes in Computer Science, Vol.1403, pp.576–589 (1998)
2. W. Ogata and K. Kurosawa, "Provably Secure Metering Scheme," Proc. of Asiacrypt 2000, Lecture Notes in Computer Science, Vol.1976, pp.388–398 (2000)
3. B. Masucci, D. R. Stinson, "Efficient Metering Schemes with Pricing," IEEE Trans. on IT, Vol.47, pp.2835–2844 (2001)

4. A. De Bonis, B. Masucci, "An Information Theoretic Approach to Metering Scheme," Proc. of ISIT 2000, p.49 (2000)
5. G.J. Simmons, "A Game Theoretical Model of Digital Message Authentication" Comgressus Numerantium, Vol.34, pp.413–424 (1982)
6. G.J. Simmons, "Message authentication with arbitration of transmitter/receiver disputes," Proc. of Eurocrypt '87, pp.151–165 (1988)
7. G.J. Simmons, "A Cartesian Product Construction for Unconditionally Secure Authentication Codes that Permit Arbitration," Journal of Cryptology, Vol.2, No.2, pp.77–104 (1990)
8. Y. Wang, R. Safavi-Naini and D. Pei, "Combinatorial Characterisation of l-Optimal Authentication Codes with Arbitration," J. of Combinatorial Mathematics and Combinatorial Computing, Vol.37, pp.205–224 (2001)
9. T. Johansson, "On the construction of perfect authentication codes that permit arbitration," Proc. of Crypto '93, Lecture Notes in Computer Science, Vol.773, pp.343–354 (1993)
10. T. Johansson, "Lower Bounds on the Probability of Deception in Authentication with Arbitration," IEEE Trans. on Information Theory, Vol.40, pp.1573–1585 (1994)

A Bounds for Multiple-use A^2-code by Wang et al.

Wang, Safavi-Naini and Pei defined the cheating probabilities of k-multiple-use A^2-codes as follows, where $\tilde{P}_t$, $\tilde{P}_{r_i}$ and $\tilde{P}_{o_i}$ denote the cheating probabilities by $\mathcal{T}$, $\mathcal{R}$ and $\mathcal{O}$, respectively.

$$\tilde{P}_t \stackrel{\triangle}{=} \max_{e_t}\left(\max_{m=(s,a),a\neq e_t(s)} \Pr(e_r(s,a)=1)\right)$$

$$\tilde{P}_{r_i} \stackrel{\triangle}{=} \max_{e_r}\max_{m_1,\ldots,m_i}\left(\max_{(s',a')\notin\{m_1,\ldots,m_i\}} \Pr(a'=e_t(s') \mid \mathcal{T} \text{ sent } m_1,\ldots,m_i)\right)$$

$$\tilde{P}_{o_i} \stackrel{\triangle}{=} \max_{m_1,\ldots,m_i}\left(\max_{m'\notin\{m_1,\ldots,m_i\}} \Pr(\mathcal{R} \text{ accepts } m' \mid \mathcal{T} \text{ sent } m_1,\ldots,m_i)\right).$$

They then showed a lower bound on the cheating probabilities and the size of keys as follows.

Proposition 2. *[8, Theorem 3.1, 3.2, 3.3]*

$$\tilde{P}_t \geq 2^{H(\hat{E}_r|\hat{M},\hat{E}_t)-H(\hat{E}_r|\hat{E}_t)}$$
$$\tilde{P}_{r_i} \geq 2^{-H(\hat{E}_t|\hat{M}_1\cdots\hat{M}_i,\hat{E}_r)+H(\hat{E}_t|\hat{M}_1\cdots\hat{M}_{i+1},\hat{E}_r)}$$
$$\tilde{P}_{o_i} \geq 2^{-H(\hat{E}_r|\hat{M}_1\cdots\hat{M}_i)+H(\hat{E}_r|\hat{M}_1\cdots\hat{M}_{i+1})}$$

Proposition 3. *[8, Theorem 4.1, 4.2] If $\tilde{P}_{o_i}$ and $\tilde{P}_{r_i}$ achieve their lower bounds, then*

$$|E_t| \geq 1/\textstyle\prod_{i=0}^{k-1}(\tilde{P}_{o_i}\tilde{P}_{r_i}). \qquad (6)$$

If $\tilde{P}_{o_i}, \tilde{P}_{r_i}, 0 \leq i < k$, and $\tilde{P}_t$ achieve their lower bounds, and the equality of eq.(6) holds, then

$$|E_r| \geq 1/\tilde{P}_t\textstyle\prod_{i=0}^{k-1}\tilde{P}_{o_i}.$$

B Construction of Multiple-use A^2-codes

Wang et al. showed that there exists a k-multiple-use A^2-code if there exists a certain combinatorial design [8]. However, they did not show an explicit construction of that design. Therefore, no explicit construction of k-multiple-use A^2-code is known.

By substituting the modified Ogata-Kurosawa metering scheme into the proof of Theorem 6, we immediately obtain an explicit construction of a k-multiple-use A^2-code as follows.

Let p be a large prime number.

Initialization Phase: An arbiter $\mathcal{A}'$ chooses a random number $r \in Z_p$ and two random polynomials $f_0(y)$ and $f_1(y)$ with degree at most $k-1$ over $GF(p)$. Let $e_t = (f_0(y), f_1(y))$ and $e_r = (r, g(y))$, where $g(y) = f_0(y) + rf_1(y)$. Then $\mathcal{A}'$ gives e_t to $\mathcal{T}$ and e_r to $\mathcal{R}$ secretly as their secret keys.

Communication Phase: For a source state $s \in Z_p$, $\mathcal{T}$ sends $m = (s, f_0(s), f_1(s))$ to $\mathcal{R}$. $\mathcal{R}$ accepts $m = (s, a, b)$ as authentic iff $g(s) = a + rb$.

Dispute Phase: On dispute between $\mathcal{T}$ and $\mathcal{R}$, $\mathcal{A}'$ accepts $m = (s, a, b)$ as authentic iff $f_0(s) = a$ and $f_1(s) = b$.

It is clear that $|E_t| = p^{2k}, |E_r| = p^{k+1}, |A| = p^2$. From eq.(3) and Theorem 6, it holds that $P_T = 1/p, P_R \leq 1/p, P_O = 1/p$. More than that, we can show the following lemma.

Lemma 7. *In the above k-multiple-use A^2-code, $P_R = 1/p$.*

Proof. $\mathcal{R}$ has a secret key $e_r = (r, g(y))$, where $g(y) = f_0(y) + rf_1(y)$ for some $f_0(y)$ and $f_1(y)$ with degree at most $k-1$. Suppose that $\mathcal{R}$ received $m_1 = (s_1, a_1), \ldots, m_l = (s_l, a_l)$. Let

$$F_0 \overset{\triangle}{=} \{(f_0(y), f_1(y)) \mid g(y) = f_0(y) + rf_1(y),$$
$$\text{where } \deg f_0(y) \leq k-1, \deg f_1(y) \leq k-1\},$$
$$F_1 \overset{\triangle}{=} \{(f_0(y), f_1(y)) \mid a_1 = (f_0(s_1), f_1(s_1)), \ldots, a_l = (f_0(s_l), f_1(s_l))\}.$$

Then $\mathcal{R}$ knows that $e_t \in F_0 \cap F_1$.

Next suppose that $\mathcal{R}$ claims that she received (s', a') such that $s' \notin \{s_1, \ldots, s_l\}$. If m' could be made by $\mathcal{T}$, then $a' = (f_0(s'), f_1(s'))$. Let

$$F_2 \overset{\triangle}{=} \{(f_0(y), f_1(y)) \mid a' = (f_0(s'), f_1(s'))\}.$$

Then,

$$\begin{aligned} \Pr(a' = e_t(s')) &= |F_0 \cap F_1 \cap F_2| / |F_0 \cap F_1| \\ &= p^{k-l-1}/p^{k-l} \\ &= 1/p. \end{aligned}$$

□

Then we see that our multiple-use A^2-code is optimum and Theorem 5 is tight because our multiple-use A^2-code satisfies all the equalities of Theorem 5.